Cognitive INFOSEC

Dr. Joseph Mitola III

US Department of Defense, 3701 North Fairfax Drive, Fairfax, VA 22203, USA

Abstract — **This paper characterizes technology challenges of Cognitive Information Security (INFOSEC). This far-term vision re-invents software radio as a "trusted" cognitive agent for the consumer or the military. Cognitive radio (CR) is software radio employing cognition technology to enhance information services for the user. Cognitive INFOSEC (CI) employs the cognition technology to achieve a high level of trust. Hardware needs for CI are substantially more demanding than for software radio. CI hardware includes non-RF sensors such as binaural audio, stereo video, biometrics and accelerometers. CR also needs multiband, multimode RF capabilities. This leads to interesting new microwave hardware design tradeoffs. Cognition sensors may share System on Chip (SoC) subsystems with INFOSEC hardware, location-awareness sensors, and RF hardware in wearable formats. This paper provides far-term concepts of operations, suggesting new SoC tradeoffs and related technology challenges.**

I. Introduction

Cognitive radio (CR) includes robust computational models of the radio itself, the user, the network, and the RF propagation environment [1]. As illustrated in Fig. 1, the attainment of cognition may be structured as a sequence of increasingly model-based, autonomously acquired reasoning capabilities ranging from the simple goal-driven behavior of today's best software-defined radios towards increasingly human-like competence to know, understand, earn INFOSEC trust, and to adaptively support the user. To achieve such levels of cognition requires novel sensors, increased signal processing, and tighter integration in small, ultimately wearable formats.

Underlying and enabling these advances will be breakthroughs in sensors, sensor-level preprocessing, machine perception, pre-cognitive cross-sensor correlation, knowledge representation, and machine learning. The integration of machine perception and planning technologies into software radio will enable adaptive behavior, including adapting to the user, location and local environment. Planning also enables negotiation, e.g. across candidate networks or service providers. Thus, CR entails the ability to extract natural language from natural acoustic backgrounds, to parse discourse, and to infer the user's information needs from the inferred user state.

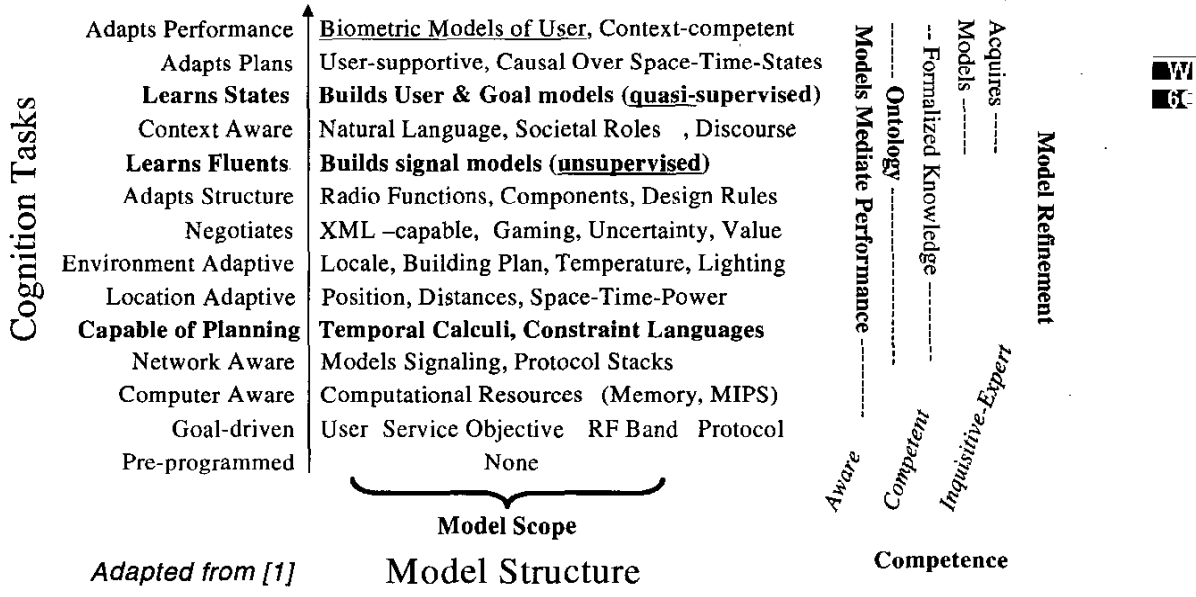


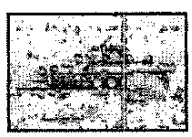
Fig. 1. Cognition technology includes model-based awareness, machine-learning, and adaptation [2].

0-7803-7695-1/03/$17.00 © 2003 IEEE

A-priori ontology [3] should express sufficient general world knowledge to enable the sharing of knowledge. Machine learning then must bootstrap user-, location-, and situation-specific models. User-supportive reasoning over space, time, user-state, and communications opportunities may then be synthesized based on a rich suite of sensory inputs.

Therefore, machine learning advances are needed both in the way algorithms characterize temporal flows of sensor signal streams ("fluents") [4] and in the way precepts are formed and manipulated in the discovery and seeking of goals [5]. Cognitive radio requires next-generation user-state awareness, the ability to adapt to not just location, but to the inferred state of the user in that location.

For the user to delegate important information transactions to a CR, the computational device must be "trusted." Trust goes beyond conventional INFOSEC features of authentication, anti-tamper, privacy, assured service, and non-repudiation. Any single biometric sensor is unlikely to establish sufficiently user-friendly and repeatable authentication to proliferate in consumer markets, in spite of market pull from proliferating thefts of laptops and PDAs. This is so because virtually any single-mode biometric sensor can be spoofed. More important, such biometric sensors must be calibrated and managed, which is problematic for the consumer. Truly unique biometrics like fingerprints and retinal images cannot be changed (like a password can) if stolen. Thus, the trustworthiness of a computational agent for CI seems inherently bound up with the difficulties of biometrics.



Effectors
Speech Synthesizer
Text Display
RF Band/ Mode Control

RF Bands and Modes
GSM (IS-136, etc)
GPRS (UWC-136 ...)
3G (W-CDMA ...)
RF LAN
AM Broadcast
FM Broadcast
NOAA Weather
Police, Fire, etc.

Environment Sensors
Location:
GPS (Glonass, Loran, ...)
Accelerometer, INS/IMU
Magnetometers (North)
Relative Positioning:
Local Broadcast
(Nodes, Range-finders)
Timing:
Precision Clock
GPS Clock Updates
Other:
Ambient Light Meter
Temperature Sensor

Local Sensors
Speech ID & Recognition
Video, Image Recognition
Keyboard, Buttons

Fig. 2. Potential Cognitive Radio and INFOSEC Sensors.

To enhance consumer acceptance, "trust" needed for CI could be derived from multi-sensory stimuli, such as those illustrated in Fig. 2. The multi-sensory sensors may be integrated into the PDA or the military vehicle. The stimuli must be parsed and integrated over time to create a deeper, more personal level of recognition of the user, location, and situation. Relevant research includes biometric person authentication via audio and video [6]. Such technologies might create a depth of recognition both more assured and less troublesome to consumers than conventional biometrics. Cognitive authentication could become a gateway to non-repudiation, privacy and other information assurance aspects of CI. Sight and sound, together with temperature, GPS, and inertial navigation sensors to interpret and validate the sight and sound stimuli might be the enablers for CI as a future "killer application". A scenario of a cognitive PDA employing CI sets the framework for microwave technology and architecture tradeoffs.

II. CI Concept of Operations (CONOPS)

Consider the following CI CONOPS, a scenario describing how the devices of Fig. 2 should function. A future military software radio, such as the Joint Tactical Radio System (JTRS) "after-next" or an Nth G commercial PDA has cognition capabilities. It knows its name is Hugo and it is "Joe's PDA". Hugo, the Cognitive Wireless PDA (CW-PDA), falls off Joe's belt-clip as Joe gets into his SUV. Hugo detects the hard bounce off the pavement, so it synthesizes "HELP!" Joe does not hear this because the SUV door is closed. Hugo also knows it was on the way from the Hotel to the Office, because it was paying attention when Joe said to Lynne' "I have to go back to the Office for an hour."

Hugo evaluates available RF communications bands and modes, with the goal of getting back onto Joe's belt, satisfying one of its basic needs. It pages Joe's Blackberry III wearable pager with "I fell off your belt near the SUV." Joe clicks "OK." Hugo hears an SUV approach, paging the Blackberry with "I am near the curb," which it determined from image processing. It hears a ping from Homer, the Cognitive SUV's CR personality.

Hugo detects motion in its video sensor, so it beeps. Somebody picks it up. Hugo looks at this person and determines that this is probably (90%) not Joe. The image is wrong. "Who are you?" it asks. "I'm Charlie," the person answers. Hugo now has a 99% probability that this is not Joe. "Do you see a Honda SUV around here? I fell out," Hugo says, not offering his name. Charlie says "Sure, its across the street." "Could you take me there?"

If Charlie says "Sure," and walks to the SUV, all is well. If Charlie says "Sure," and stuffs the PDA in his

pocket, walking off in the other direction, the PDA should change "user state" to "theft-event." The PDA needs inertial navigation sensors since GPS is not consistent in this urban canyon.

Hugo warns Charlie at highest volume "You are heading in the wrong direction. I think you are trying to steal me. Please stop." Charlie, a hardened criminal, throws Hugo in the trunk of his car. Ten minutes later, Charlie arrives home, and pulls Hugo out of his trunk. Hugo says, "I will call the police," so Charlie hits the power-off button. Hugo's CI module detects power-down, and stops talking. The CI module's low power long-endurance battery never turns off. Hugo thus transmits an emergency message <Theft, Urgency, Location, Thief.jpg>. The theft message has a processing gain of 10,000, picked up by a nearby police car on VHF. The urgency code indicates Hugo's value. Hugo's location is displayed on the city map in the police car. Hugo transmitted a full-face view of the thief, taken when Charlie picked up Hugo.

Charlie tries to unscrew Hugo's back, but the interior locking pins retain the screws. Only Hugo can release those pins and only if he knows he is with Joe or a CR specialist, at a CI-authenticated CR assistance location.

The knock at the door startles Charlie. "Yes?" "Police," Officer Black replies. "What do you want?" "We have a warrant to search these premises based on an emergency report from a CW-PDA," Black replies. Charlie is on his way to jail in this scenario.

In other scenarios, Charlie succeeds in removing Hugo's back and tries to obtain Joe's personal information, Hugo's other Information Assurance (IA) features emerge. Would Hugo have erased all of Joe's personal data? Suppose the batteries are going dead? A PDA with dead batteries will not be very resistive of illicit attempts to extract information, so long-endurance power is needed for CI. When Hugo was thrown into the trunk of a car, how did it know where the thief was taking it without GPS? People who are kidnapped sometimes remember sounds, associating them with motion, such as the crossing of a railroad tracks, or hearing the whistle of a fog horn. Would such measures, along with MEMS inertial navigation help Hugo accurately pinpoint its location in urban canyons? Theft of laptop computers and identities continues to climb. Will networks emerge to which Hugo could interact to avert identify theft? Could there be a future 911 for cognitive devices?

In a military setting, the user might be a casualty, wounded in battle. Should Hugo radio for a medic if Joe suddenly slumps over and biometrics indicate trauma? Should Hugo behave like Joe's comrade in arms? If Hugo is captured, can he assert protection under the Geneva Convention as a "US Person?" There seem to be many alternatives to hard erasure of all data that would be beneficial to users. The preceding sets a useful backdrop. Parsing this illustrative CONOPS yields Table 1.

Table 1 Sensing Capabilities Derived from CONOPS

State or State Transition	Sources, Sensors, or Perception
Name is Hugo	Speech and text
Identity: Joe's PDA (from bonding over time)	Voice speaker identification Video face isolation & recognition
On Joe's belt clip	Clip tension, temperature, RF multipath
Falling from Joe's belt clip	Clip tension, Δ temp, video flow
Hitting pavement	Shock signature, RF attenuation
Located at Hotel	Prior GPS, RF bands profile, images
Walking to parking lot	Intermittent GPS, light level, images
On the way to work	Interpreted Lynne's ambient speech
Paging Blackberry III	Reliability of RF bands, modes
Detects Homer	Homer's RF beacon, acoustics
In User's Hand	Exterior shell pressure sensors, temp
Unknown user	Face isolation, speaker identification
Theft	Inertial sensors, light level, acoustics
Attempt to remove cover	Torsion on locking pins, shock profile
Location report to police	Intermittent GPS plus integration of inertial sensors over time

Consider the hardware challenges implicit in this table.

III. Microwave Technology Challenges

Microwave hardware and architectures must evolve substantially to enable sensor-rich but cost-effective CW-PDA devices like Hugo.

A. Conventional Components and Architectures

Increasingly, conventional cellular handsets and PDAs incorporate camera sensors [7], laying a foundation for Hugo. Current architectures may be characterized as parallel multimedia dominated by a voice-RF-voice thread (in bold lines), illustrated in Fig 3.

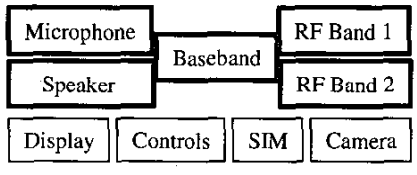


Fig. 3. Conventional Voice-Dominated Phone

GSM architectures feature the Subscriber Identity Module (SIM). This INFOSEC module provides mutual authentication between the handset and the network, with stream encryption for privacy. SIM cards may be transferred among GSM phones, moving the subscriber identity from one handset to another. Should future CW-PDA architectures permit similar hardware-based mobility of a subscriber's personality? Of the C-PDA's personality?

B. Cognitive Components and Architectures

The increased hardware complexity of future CW-PDAs begins to emerge as one considers the diversity of sensors implicit in Fig 4.

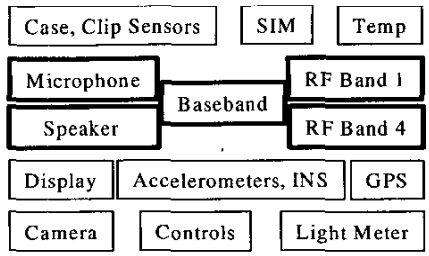


Fig. 4. Future Cognitive PDA Architecture

In this vision of the future, the voice-RF thread is still present, but less dominant. The four RF bands access RF LAN and VHF in addition to two cellular bands. Underlying and integrated into sensors, controls, and RF are many ADCs, DACs, clocks, digital processors and memory. Might future microwave hardware be partitioned and integrated into the sensor suites? For example, could a video-capable ADC support both camera and RF functions in a time-shared architecture? What about SoC multi-antenna beamforming, stereo optics and binaural signal processing? How tightly should sensors in the PDA's case be integrated into the rest of the architecture? Should sensors share case-skin with antenna apertures?

C. Cognitive INFOSEC Architectures

In addition to a future SIM card, the INFOSEC features of the CW-PDA include multi-sensor inputs. Sensors in the case protect the device from physical tampering. Not as obvious from the hardware block diagram are the contributions of acoustic, video, accelerometer/ Inertial Navigation Subsystem (INS), light meter, GPS, and temperature sensors to cognitive INFOSEC through perception and machine learning.

Thus, one must ask whether traditional INFOSEC features, like mutual authentication, might be integrated more fully into these non-INFOSEC components. For example, should today's plug-and-play hardware-software standards be extended to plug-authenticate-and-play? If not, then it could be too easy for a thief to spoof the CW-PDA's sensors. Should plug-in modules include digital signatures, perhaps? Could the CW-PDA compare authentication data from a trusted wireless network with the digital signature of a plug-in? Such approaches seem more secure, but also could inhibit the usefulness of the CW-PDA in situations where the device cannot access the network, such as in many military situations.

How could the CW-PDA integrate across its multi-sensor suite to infer the voracity of the individual sensory inputs? Multi-sensor measures, such as correlating spatial balance against video flow are used by biological systems to achieve orientation. How could Hugo orient? How can it know when to unlock the locking pins, to allow Joe to insert or remove hardware, while not allowing either Charlie the thief or Joe under duress from Charlie to start to take it apart? In short, what is the architecture by which sensors and actuators should be controlled by Hugo's CI element and supported by Hugo's multi-sensor suite?

IV. Conclusions

This brief treatment characterized the evolution of commercial and military cell phone technology towards Hugo, the sensor-rich CW-PDA. Since this technology is just on the horizon, the purpose was to present a vision and to pose questions that may help cost- and value-effective microwave technologies for CW-PDA to emerge.

References

[1] J. Mitola III, *Cognitive Radio, Doctoral Dissertation*, Stockholm: KTH, The Royal Institute of Technology.

[2] J. Neel, J. Reed, and R. Gilles, "The Role Of Game Theory In The Analysis Of Software Radio Networks," *Proc. SDR Forum Technical Symposium,* Rome, NY: SDR Forum, Nov 2002

[3] B. Kettler, "DARPA Control of Agent Based Systems (CoABS) Program, The CoABS Grid: Technical Vision" www.isx.com: ISX Corporation, 9/30/01 (Version 2.3).

[4] P. Cohen, "Neo: Learning Conceptual Knowledge by Sensorimotor Interaction with the Environment" *Proceedings, Autonomous Agents 97 (ACM)* 1997.

[5] R. Sun and T. Peterson, "Some experiments with a hybrid model for learning sequential decision making" *Information Sciences 111 83-07,* Amsterdam, The Netherlands: Elsevier, 1998.

[6] 4th International Conference on Audio- And Video-Based Biometric Person Authentication, Call for Papers, Surrey, UK: www.apds.com, 2003

[7] 'MotoMomentum' (E365 GSM camera handset) Shanghai, China: www.motorola.com/mediacenter/news/ 2003